2021长安“战疫”网络安全卫士守护赛 misc部分writeup

原创

shu天 于 2022-01-13 19:45:58 发布 113 收藏

分类专栏： # misc ctf 文章标签： ctf misc

不允许转载

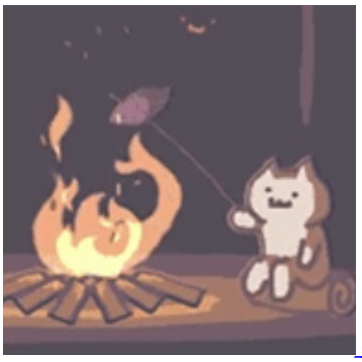
本文链接：https://blog.csdn.net/weixin_46081055/article/details/122378940

版权

misc 同时被 2 个专栏收录

7 篇文章 0 订阅

订阅专栏



ctf

81 篇文章 4 订阅

订阅专栏

2021长安“战疫”网络安全卫士守护赛 misc部分writeup

八卦迷宫

朴实无华的取证

西安加油

ez_Encrypt

一百多名，我觉得还行欸，多亏了队里的crypto手

八卦迷宫

签到题，走迷宫，换成字就可以了

朴实无华的取证

老规矩先看pslist

```
D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\download\xp_sp3\xp_sp3.raw)
                      PAE type : PAE
                           DTB : 0x764000L
                          KDBG : 0x8054e2e0L
          Number of Processors : 2
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
                KPCR for CPU 1 : 0xf8757000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-12-27 02:37:41 UTC+0000
     Image local date and time : 2021-12-27 10:37:41 +0800

D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 pslist > 1\ps/txt
系统找不到指定的路径。

D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 pslist > 1\ps.txt
Volatility Foundation Volatility Framework 2.6

D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 filescan > 1\file.txt
Volatility Foundation Volatility Framework 2.6
```

CSDN @shu天

进程里面有 文本查看器，360压缩和图片查看器

ps.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
0x81c47308 svchost.exe            3488    712      5      128      0      0 2021-12-27 01:40:27 UTC+0000
0x81fd27e8 softupnotify.ex        2936    916      0 --------      0      0 2021-12-27 01:40:40 UTC+0000   2021-12-27 01:40:40 UTC
+0000
0x819b0970 mspaint.exe            3888   1904      9      258      0      0 2021-12-27 01:44:37 UTC+0000
0x81a08da0 conime.exe             3260   2124      9      183      0      0 2021-12-27 01:44:47 UTC+0000
0x81d68a50 IEXPLORE.EXE           3748   1904     21      578      0      0 2021-12-27 01:44:52 UTC+0000
0x819d6a18 wdswfsafe.exe          2136    916      4       70      0      0 2021-12-27 01:44:52 UTC+0000
0x819c98a0 softupnotify.ex         884    916      0 --------      0      0 2021-12-27 01:44:52 UTC+0000   2021-12-27 01:44:52 UTC
+0000
0x81c2b2f0 IEXPLORE.EXE           3976   3748     37     1374      0      0 2021-12-27 01:44:52 UTC+0000
0x819b23b0 softupnotify.ex        1916    916      0 --------      0      0 2021-12-27 02:00:18 UTC+0000   2021-12-27 02:00:18 UTC
+0000
0x81c33630 softupnotify.ex         972    916      0 --------      0      0 2021-12-27 02:03:28 UTC+0000   2021-12-27 02:03:28 UTC
+0000
0x81f2c7e0 notepad.exe            2976   1904      6      180      0      0 2021-12-27 02:27:06 UTC+0000
0x81c7f630 360zip.exe             3388   1904     10      366      0      0 2021-12-27 02:28:39 UTC+0000
0x81d4d020 2345PicViewer.e        3812   1904     23      378      0      0 2021-12-27 02:36:41 UTC+0000
0x81923020 taskmgr.exe            3628    668      9      188      0      0 2021-12-27 02:37:11 UTC+0000
0x81c30da0 DumpIt.exe             3300   1904      1       16      0      0 2021-12-27 02:37:38 UTC+0000
```

CSDN @shu天

cmd运行过的程序也可以印证，发现有flag.zip和flag.png

```
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 cmdline
```

```
**************************************************
IEXPLORE.EXE pid:   3976
Command line : "C:\Program Files\Internet Explorer\IEXPLORE.EXE" SCODEF:3748 CREDAT:79873
**************************************************
softupnotify.ex pid:   1916
**************************************************
softupnotify.ex pid:    972
**************************************************
notepad.exe pid:   2976
Command line : "C:\WINDOWS\system32\NOTEPAD.EXE" C:\Documents and Settings\Administrator\妗岍潰\鎴戠殑鏃ヨ  .txt.txt
**************************************************
360zip.exe pid:   3388
Command line : "C:\Program Files\360\360zip\360zip.exe"  "C:\Documents and Settings\Administrator\妗岍潰\flag.zip"
**************************************************
2345PicViewer.e pid:   3812
Command line : "C:\Program Files\2345Soft\2345Pic\2345PicViewer.exe"  "C:\Documents and Settings\Administrator\妗岍潰\flag.png"
**************************************************
taskmgr.exe pid:   3628
Command line : taskmgr.exe
**************************************************
DumpIt.exe pid:   3300
Command line : "D:\360瀹夊叏娴忚鍣  鍚尤笈杞絓DumpIt\DumpIt.exe"
```

CSDN @shu天

filescan取出flag.zip和flag.png

```
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000
0000017ad6a8 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x017ad6a8   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\妗岍潰\flag.z
ip
SharedCacheMap 0x017ad6a8   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\妗岍潰\flag.zip

λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000
000001e65028 -D ./ -n
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x01e65028   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\妗岍潰\flag.p
ng
```

flag.zip导出有损坏，可以winrar用自带的修复

CSDN @shu天

密码是在记事本里面`20211209`

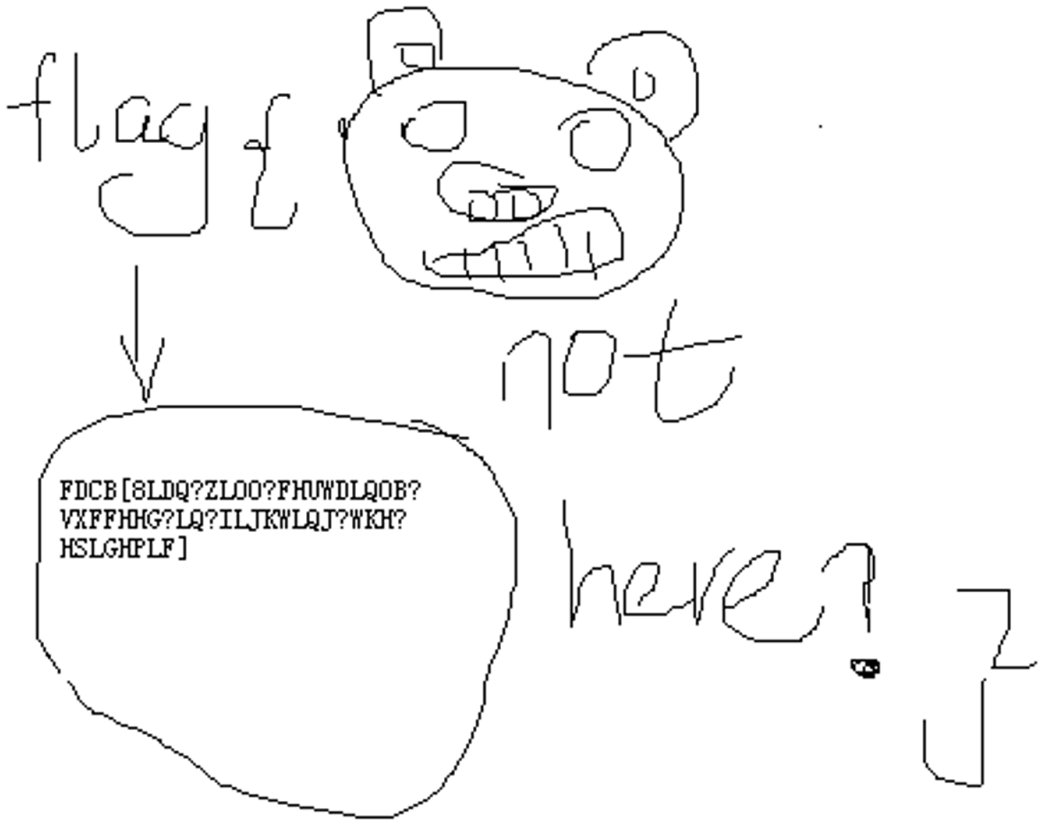
```
D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 notepad
Volatility Foundation Volatility Framework 2.6
Process: 2976
Text:
?

Text:
?

Text:
L

Text:
?

Text:
??????????????
20211209(encrypt)
????????????????????????
????!?????
????!???
```

CSDN @shu天

encrypt.txt的内容

```
//幼儿园水平的加密（部分）
void Encrypt(string& str)
{
 for(int i = 0; i < str.length(); i++)
 {
  if(str[i] >='a'&& str[i]<='w')
   str[i]+=3;
  else if(str[i]=='x')
   str[i]='a';
  else if(str[i]=='y')
   str[i]='b';
  else if(str[i]=='z')
   str[i]='c';
  else if(str[i]=='_')
   str[i]='|';
  str[i] -= 32;
 }
}
```

flag.png内容



CSDN @shu天

```
FDCB[8LDQ?ZLOO?FHUHDLQOB?VXFFHHG?LQ?ILJKWLQJ?WKH?HSLGHPLF]
```

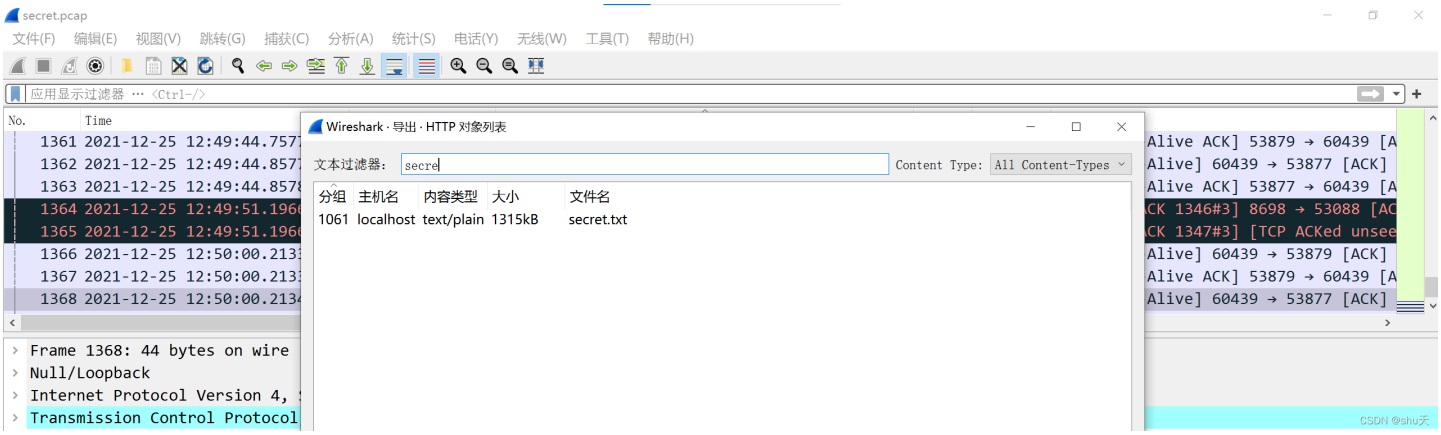
解密脚本

```
e = "FDCB[8LDQ?ZLOO?FHUHDLQOB?VXFFHHG?LQ?ILJKWLQJ?WKH?HSLGHPLF]"
d = ""
for i in e:
    i = chr(ord(i)+32)
    if 'd'<=i<='z':
        i = chr(ord(i)-3)
    elif i=='a':
        i='x'
    elif i=='b':
        i='y'
    elif i=='c':
        i='z'
    elif i=='|':
        i=='_'
    d += i
print(d)
```

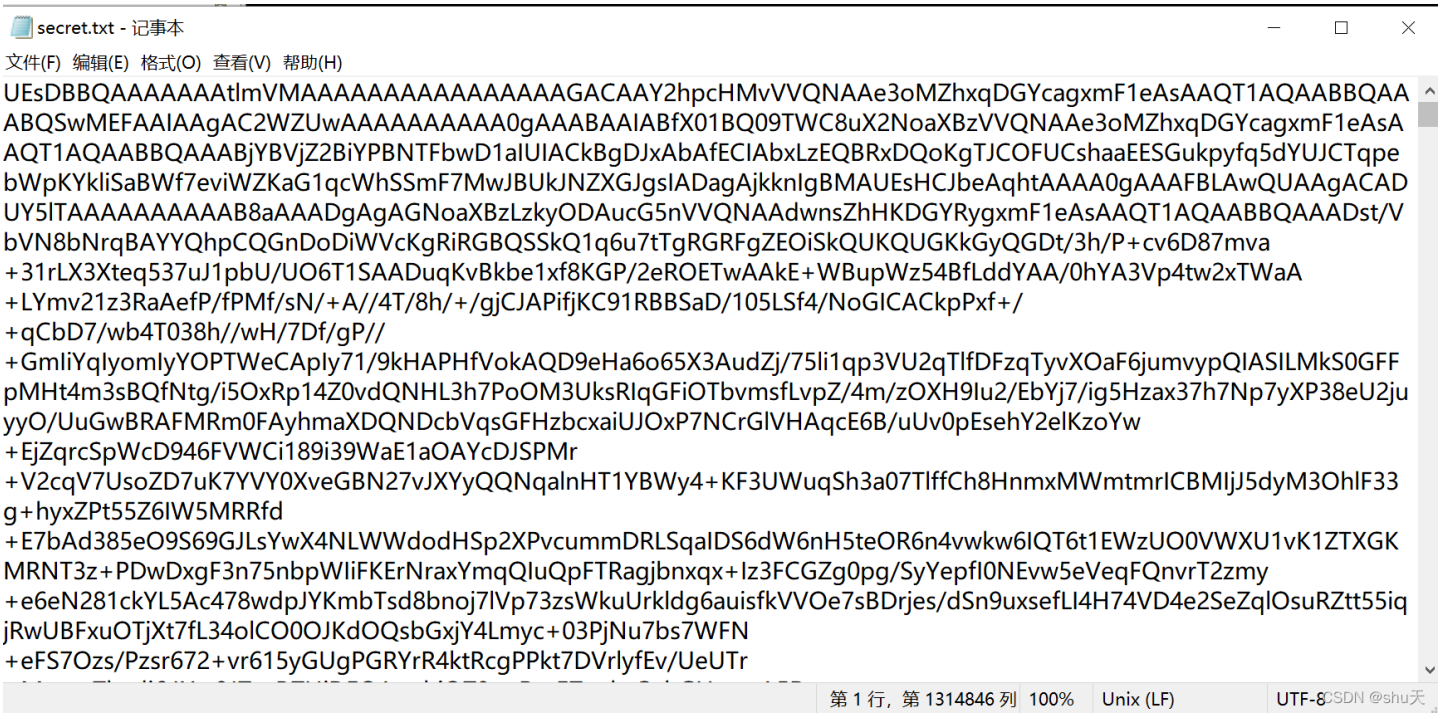
```
cazy{Xian_will_certainly_succeed_in_fighting_the_epidemic}
```

西安加油

发现http流里面有secret.txt



导出



base64解密（https://the-x.cn/base64），发现是压缩包

```
24.24KByte       chips/7079.png
172Byte __MACOSX/chips/._7079.png
27.78KByte       chips/5444.png
172Byte __MACOSX/chips/._5444.png
28.13KByte       chips/9056.png
172Byte __MACOSX/chips/._9056.png
23.33KByte       chips/3195.png
172Byte __MACOSX/chips/._3195.png
17.41KByte       chips/7683.png
172Byte __MACOSX/chips/._7683.png
27.06KByte       chips/4365.png
172Byte __MACOSX/chips/._4365.png
10.00KByte       chips/.DS_Store
120Byte __MACOSX/chips/._.DS_Store
21.25KByte       chips/7321.png
172Byte __MACOSX/chips/._7321.png
17.42KByte       chips/1220.png
172Byte __MACOSX/chips/._1220.png
```

插件【Zip】Zip-based or zip file
另存为：**zip文件**
附加信息：

```
Encrypted:false
Files:100
Total Size:1182014
```

显示内容非原始信息
数据长度：*986,604 Bytes*
插件数：*18*，耗时：*22ms*

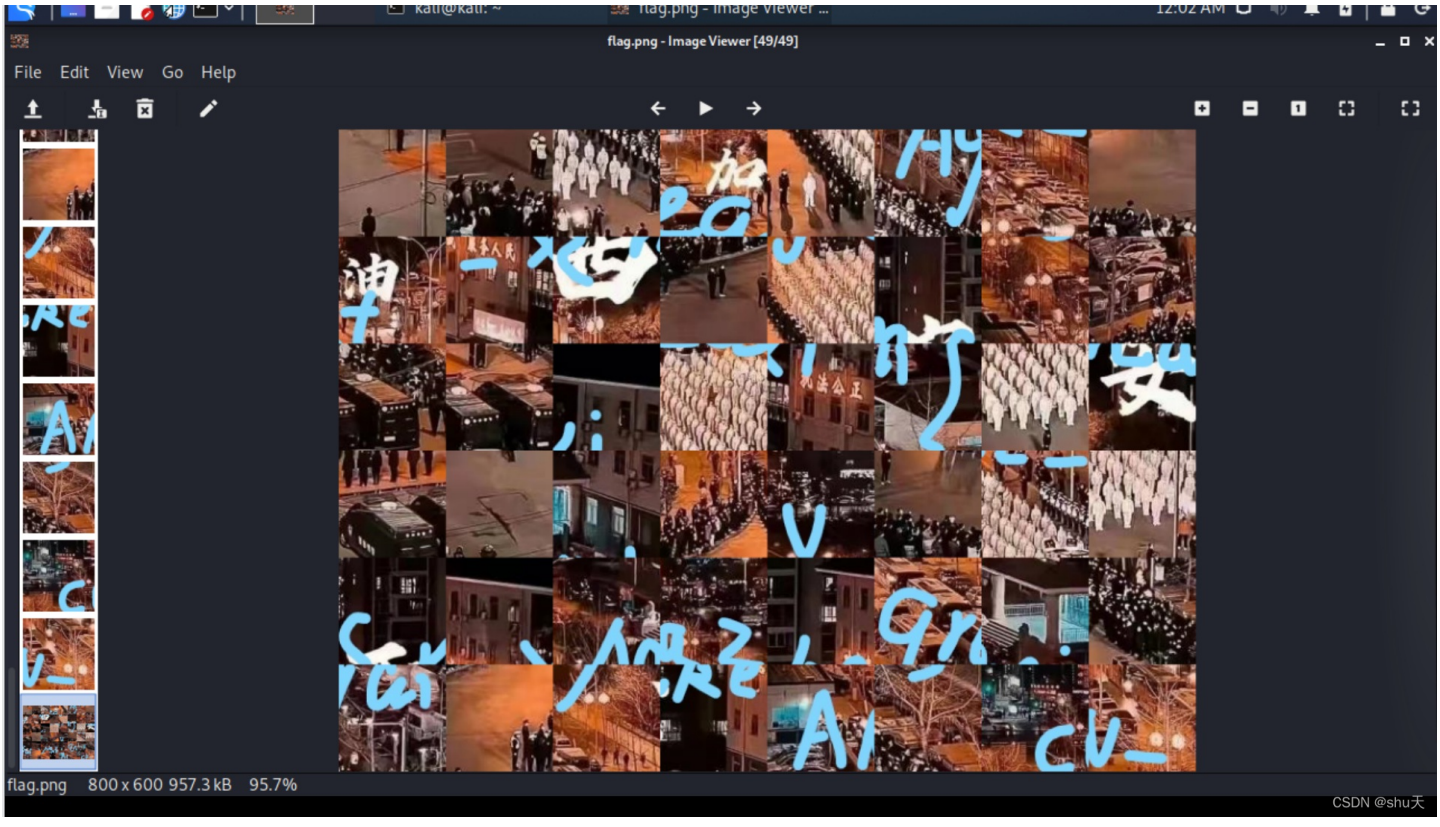
CSDN @shu天

里面是一堆图片，看起来是要拼图

> montage和gap安装使用时参考的博客
> https://blog.csdn.net/m0_47643893/article/details/113778577
> https://www.cnblogs.com/bhxdn/p/14094717.html
> https://github.com/nemanja-m/gaps

先把图片合成一张

```
sudo apt-get install montage
montage *.png -tile 8x6 -geometry +0+0 flag.png
```

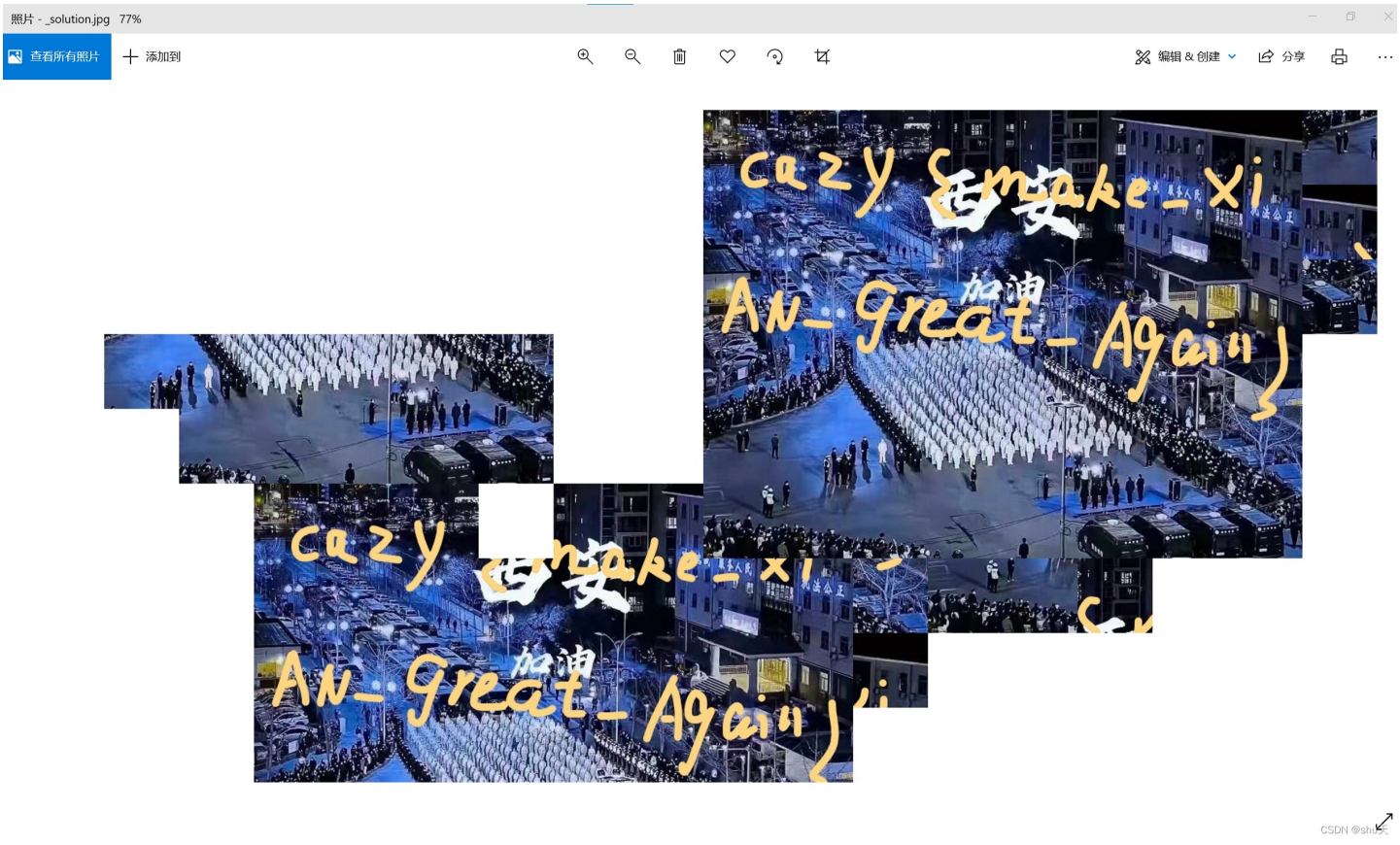


然后用gaps拼图

```
gaps --image=../flag.png --size=100 --save
```

```
p3@p3-virtual-machine:~/ctftool/gaps$ gaps --image=../flag.png --size=100 --save

=== Population:  200
=== Generations: 20
=== Piece size:  100 px
=== Pieces:      900

=== Analyzing image: ████████████████████████████████████████████████████ 100.0%
=== Solving puzzle:  ██████████████████████████████---------------------- 57.9%

=== GA terminated
=== There was no improvement for 10 generations

=== Done in 257.731 s
=== Result saved as '_solution.jpg'
=== Close figure to exit
p3@p3-virtual-machine:~/ctftool/gaps$
```

CSDN @shu天



`cazy{make_XiAN_great_Again}`

当时只出了三条……

ez_Encrypt

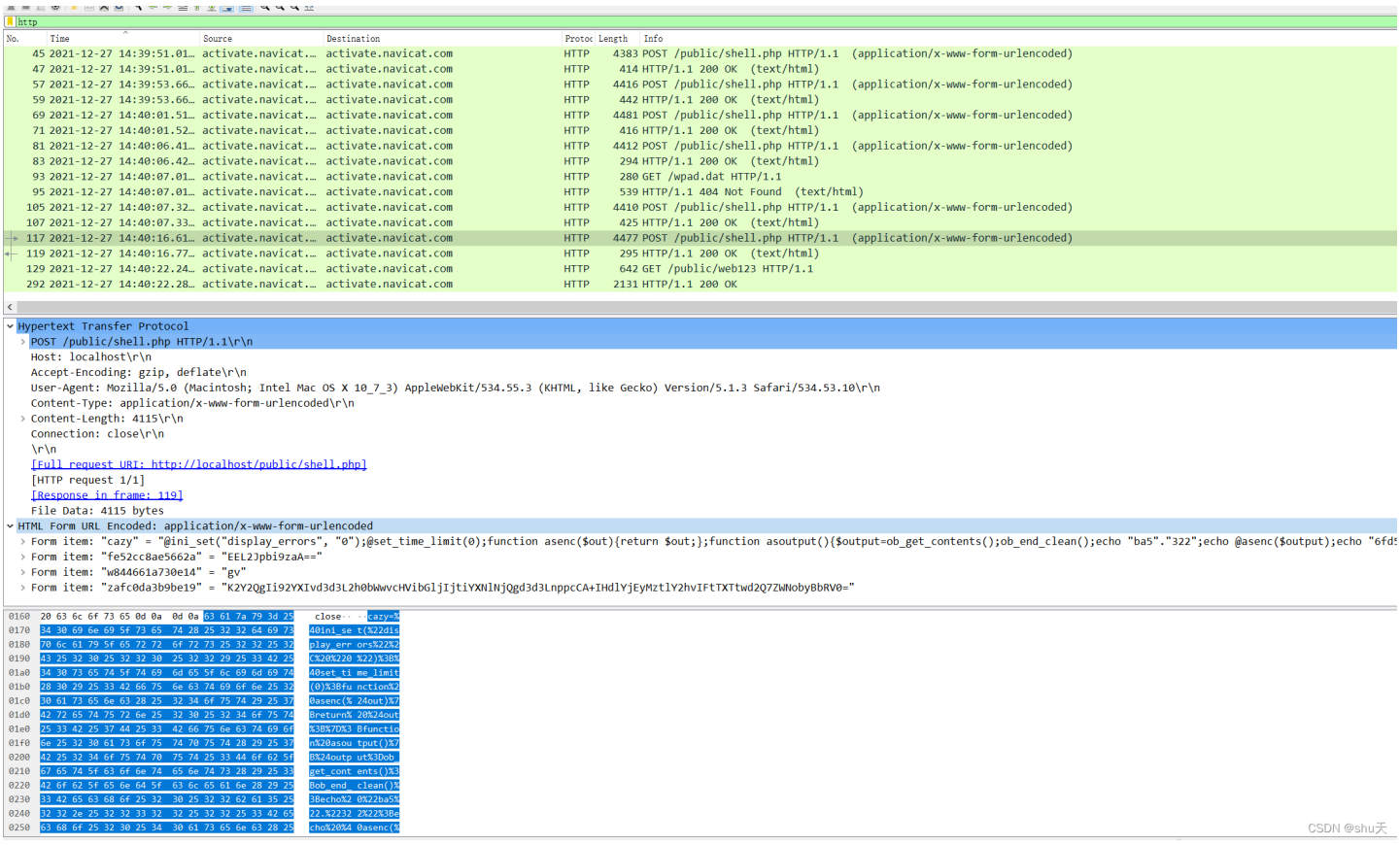
导出http流可以发现最后有个web123

```
GET /public/web123 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
If-Modified-Since: Mon, 27 Dec 2021 06:30:20 GMT
If-None-Match: "12451a-5d41ad6b87e79"

HTTP/1.1 200 OK
Date: Mon, 27 Dec 2021 06:40:22 GMT
Server: Apache/2.4.48 (Debian)
Last-Modified: Mon, 27 Dec 2021 06:40:16 GMT
ETag: "124470-5d41afa47656c"
Accept-Ranges: bytes
Content-Length: 1197168
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

UEsDBBQAAAAAAMhOmlMAAAAAAAAAAAAAAAAAAEACAAYXBwL1VUDQAHWF/JYVhfyWFYX81hdXgLAAEE
9QEAAAQUAAAAUEsDBBQACAAIAMhOmlMAAAAAAAAAANIAAAAOACAAX19NQUNPU1gvL19hcHBVVA0A
B1hfyWFYX81hb1/JYXV4CwABBPUBAAAEFAAAAGNgFWNnYGJg8E1MVvAPVohQgAKQGAMnEBsB8QIg
BvEvMRAFHENCgqBMkI4VQKyFpoQRIa6SnJ+rl1hQkJOql5takpiSWJJoFZ/t6+JZkpobWpxaFJKY
XszAkFSQk1lcYmCwgANqACOSSciAEwBQSwcIlt4CqG0AAADSAAAAUEsDBBQACAAIANkokFMAAAAA
AAAAAAABAAANACAAYXBwL2V2ZW50LnBocFVUDQAH3Tm7YY1TyWGNU81hdXgLAAEE9QEAAAQUAAAA
s7EvyCjg0tdXeLKr+8nubU/XzXqys/PZtHYgm6sotaS0KE8hmksBCNSTMvNS1BXAwNYOKhirwwWR
zMksLknNU0eRBEs4FhR45mWWqEPEgerhMh41JQVBpXk4ZFzB1qHL+OSn+6SWpeaoY5MJL8osSUWR
gTuvuDSpOLkoMwkqDZOMteYCAFBLBwhGtdZWhQAAAAABAABQSwMEFAAIAAgAxHSbUwAAAAAAAAAA
BCAAAAOAIABhcHAvLkRTX1NOb3J1VVQNAAdRX81h2lvJYVFfyWF1eAsAAQT1AQAABBQAAADtWVts
```

1 客户端 分组，1 服务器 分组，1 turn(s).

CSDN @shu天

再向上看，分析蚁 剑 命令执行的流量



```
cd "/var/www/html/public";base64 www.zip > web123;echo [S];pwd;echo [E]
```

是吧www.zip的备份base编码成web123了

转成zip

然后比赛时候我就卡住了，其实联系题目里的Encrypt，可以猜想是用了什么加密函数。
D盾扫描一下就找到了

```
# \app\controller\index.php
<?php define('IKlSux1227',__FILE__);$DusPFr=base64_decode("bjF6Yi9tYTVcdnQwaTI4LXB4dXF5KjZscmtkZzlfZWhjc3dvNCtmM
zdqZHF0d3lpT2VBY1VaTHBDdUhuYm1ndkZzZlNhUFlsTUpCTmpSVmtLeFFEVFdJcnpFb1hHaA==");$arCiCL=$DusPFr[3].$DusPFr[6].$Dus
PFr[33].$DusPFr[30];$VvUrBZ=$DusPFr[33].$DusPFr[10].$DusPFr[24].$DusPFr[10].$DusPFr[24];$DEomKk=$VvUrBZ[0].$DusP
Fr[18].$DusPFr[3].$VvUrBZ[0].$VvUrBZ[1].$DusPFr[24];$LnpnvY=$DusPFr[7].$DusPFr[13];$arCiCL.=$DusPFr[22].$DusPFr[
36].$DusPFr[29].$DusPFr[26].$DusPFr[30].$DusPFr[32].$DusPFr[35].$DusPFr[26].$DusPFr[30];eval($arCiCL("JFZDQlpRVz
0iZ29NVFFoZXFpYVVPdWJtWWZSSlNya1dObmRFc1BaR2pBS3BDVnRCSUh3REZ4Y3pYTGx2eVlUY2lVdVBuZ3BzeXFib09saGpGSVpOU3d6bU1IR3
ZEeHRrWFZhV2ZkQUpFclJLTENCUWVISjlBcGR4WUd2Vm9wTjVCdFh6WmhCdXVwWmZyY0RmM2plcmpGMnJpekxZcmNEZjN0aU1aR21qbmkwOWpITm
p1UjJzMlNFOVpHTlNRR3ZzVGZvam5oREdHcGlCME5WaE5PMmhxc0x6dVZtWjBpRXVYU3ZoT2hEVkNwQmtLTzIxMHAxazZidkdwVjJ1bk9LU1p6Wj
VKenYxU1BvaHJPMXo0ekV6cWlEVkdjMUdVVnYxQXMxU3ZVWjVzRkVrVFZaVk1iVkVMR0VqRGJCZktWMHVBek5tQXpkekZoVmtrc05ycGIxek9wRW
hwVktCdlZEV1podkVMc0JHaUdLMDlmZ1o3am1rM2JadTFWSzBaR21qbmkwOWpOS1N6Q2doWlVva0hpMEJiU0IwcWp2aFhwWjlIRlZNS2MxMHFqdm
hYcFo5SEZWTUtjRTA3amRHaGl2emRGSzBaR21qbmkwOWpOS2NLTEY0Wkdtam5pMDlqTkttQUxGNFpHbWpuaTA5ak5LZjBMRjRaR21qbmkwOWpOS2
1BTEY0Wkdtam5pMDlqTktmMExpTVpOTkdNendHc0hGaDJzc3J3aDBhYmNFMHFqdmhYcFo5SEZWTXJ5RTBxanZoWHBaOUhGVk1LTEY0WnpCRWNHMH
pDTktXekNnaDJzc3J3aDBhYmNWMHFqdmhYcFo5SEZWTWVTRTA3anYxRVVWRXZPSzBaR21qbmkwOWpOS3p6Q2doWlVva0hpMEJiY2lTenllaHR6Mj
VmelZScUhGaFpVb2tIaTBCYmNEanpDZ2haVW9rSGkwQmJjS0d6Q2doWlVva0hpMEJiY0RCekNnaFpVb2tIaTBCYmNER3pDZ2haVW9rSGkwQmJjS1
d6Q2doWlVva0hpMEJiY0tqekNnaFpVb2tIaTBCYmNLVnpDZ2haVW9rSGkwQmJjREd6Q2doWlVva0hpMEJiY0tXenkyVjJPTkFUam1rM2JadTFWZV
lnRlpWcGlWVHJSZGtOcERXa1ZFVjBSQlRlU0xoc2hOck1zTnJwcEJqT05vQlpoTmhFR05hVE9WR05HbWpaVjFUS1YwenZTVmphUEVWREZtNTVOWn
pBaHZmZXBFalZjb3JpczJyTVNFVUtoWjlWaFZqSlZ2NU16VlRBekVXZ2hOdUZPS2pwczFaS05CekJidmhTVlpWeXBWQk5SSldvVk5yTk9EV05oMV
ZkYkVoZ1ZOVUtWRXVYUHZWZHNCQlpWb3JlczIxQVBORUVoWmpCcG9yTVZCVjRwdlZWaEJ1eWhKV2tpS2pOY0JCTHoyOXRQRFlJRndaMHAxU3FHZF
ZpRkVHT0YwU0ZjQlZWUHY1RmNkU1FGWkdNYk5qZk5Eak5VMnpJc29hNGJCenFpQnpjVTFqMHNCVnZzQmphaUxFU3BOYUtGWkdNYk5qZk5Eak5VMn
pJc29hNGJCenFpQnpjVTFqMHNCVnZzQmphaUxTdGhLRXZzVkd2aDFCNXAzU3Rob3JhT1p1cGNCR0pHMmFGcDN1cVYyNXlWMHJtVUxTdGhLRXZzVk
d2aDFCNXAzV0NzMk0zZmdaa3lLOCtISjlBcGR4WUd2Vm9wTjVCdFh6ZEdOU3RiczRyY0RmM2plcmpGMnJpekxZcmNEZjN0aU1aaEJrUVBtajBITm
p1UjJzMlNFOVpHTlNRR3ZzVGZvam5oREdHcGlCME5WaE5PMmhxc0x6dVZtWjBpRXVYU3ZoT2hEVkNwQmtLTzIxMHAxazZidkdwVjJ1bk9LU1p6Wj
VKenYxU1BvaHJHc1ZaVnZtZVNMekRiRVQyT0tFRk52aGFWWmhWYm1HME9OMVROTkVPYkVFWmNOclVzS1dGekJFSWJtYU5WMEduc1ZzMXBWalZwZF
NwRm1HdXNvNUZjVmhkTm81c3NpMDlmZ1o3anYxcVYydWlGSjBaaEJrUVBtajBOS1N6Q2dodk5vOTRVd2hiU0IwcWptR3BiM3VYekVNS2MxMHFqbU
dwYjN1WHpFTUtjRTA3akVHR1YyUzRHSjBaaEJrUVBtajBOS2NLTEY0WmhCa1FQbWowTkttQUxGNFpoQmtRUG1qME5LZjBMRjRaaEJrUVBtajBOS2
1BTEY0WmhCa1FQbWowTktmMExpTVpPTkdWekJ6c0hGaE5OVnpEUHZoYmNFMHFqbUdwYjN1WHpFTXJ5RTBxam1HcGIzdVh6RU1LTEY0WlZCQkxPM3
VaTktXekNnaE5OVnpEUHZoYmNWMHFqbUdwYjN1WHpFTWVTRTA3anZCWnoyclNzSzBaaEJrUVBtajBOS3p6Q2dodk5vOTRVd2hiY2lTenllaGFiQn
pUczBZcUhGaHZObzk0VXdoYmNEanpDZ2h2Tm85NFV3aGJjS0d6Q2dodk5vOTRVd2hiY0RCekNnaHZObzk0VXdoYmNER3pDZ2h2Tm85NFV3aGJjS1
d6Q2dodk5vOTRVd2hiY0tqekNnaHZObzk0VXdoYmNLVnpDZ2h2Tm85NFV3aGJjREd6Q2dodk5vOTRVd2hiY0tXenkyVjJPTkFUanYxcVYydWlGWF
lnRlp6cHMxVnFzRGhHUERXa1ZOYTRpMmhJY2loQmJOdW5zWlZwc3ZoRUZCekZjc0d1czF1WnpWa2RjTEJnaEJqTnNpVzBob0VMR3YxQlZvcnJWaV
N5UEVFTlVaYVpObWprczB6TnBFenZHZGpnYzFmMXMxek1SQlpyaW81R1ZzRzRPREVGT1ZWRUd2ckZWTGhKVm1zcnMyU2RTVmpOY0JrS3NaR01oRW
hJTndrWmNEbTJWMEdwY0JTZFJ2Qk5ORU8wczI1dHN2RWRzRGpoVnZySnMyNU5WMmp2VkJTRFZCanZPMmFNVTJjQXlza2dwM2hmTzFWdHB2U0xpRF
NOVm1acmlzenZzMDlPUkVHRmNzamRPRFd0cDJqRWNMQmlWS1Zjc0RTdlUxQk9ob2twYlo1NXMxUjFibTFuYmRFc05FR2pPVkdORkVaZVNOdVpjM1
dLTm9ydEZvVnFpd0JpVlo1Y3NaUjFSVmpWR0VFeWhMaGZWc2hGaUJmclV3RUZORUdlc2lqTnMyU05pWkdOY3ZyQVZCVjRjRWpNVkxCR2MzV3ZPMm
EwUjJWRUZvYWhjZGhhVm9heXB2aE5VQmtOVk5oMUdKVzBGRWpzaEJHVnAyYTNzMk00U05FSXptdWdiTFd2c0RFV2N2amROObzlnaExoYVZvYXlpdm
hPUmRTaWNCa0xzaVcwYlZHSWlacnBiZFdrc0JHTWhFVEFWQldTVnNreUdFelRwMVNmaGlWWk5FamhHbUdORnMwclJkV0dWMWt5VkV6NHp2am5Hdj
FMVkJrbXNLanBWMW1BenYxTnAwNWNOb3JwaEVjS1ZCRXVic1Y1VnNWcEYxVUtoREdpYlpra09vMTRGRVNkR3Z1U2J2UzVzMXVFU05FRVZCV2lWMn
J2c0RFWnAxU2ZoaVZaTkVqaEdtR05GczByUmRXR1Yxa3lWRXo0enZFbUd2MUxWQmttc0tqcFYxbUF6djFOcDA1SE5CekZoRWNlTkJ6aGNkaGFWb2
F5aXZoVnBkVnNORUdoc29yTk5CR01iRUVTYm1mMk8za2pTVkdFemR1WmgycmNzWlZNT1ZVZVNOcnBjZGg0TkRqdEZzMXFod0VpY0VqdE9WR05zRU
9BaUJqU3BCanFzS1NaU29qRXp2MU5wMDVjR0VoWFIxa01iRXpoY2RoYVYyYXRpQlVBcEpHaXBLQmVzaVdOaVZWZFJka1NjMWprVkJoamNFbWVWQm
haaEVUMFZEajBVMUdOaFprWmJFR3BzaWp0YlZ6Tk5aaGljQmt1aURqcE5CR0lpWnJwYkVrbXNLanBWMW1laEJTVmhtanlPMmFUUlZjZU5aNVpjMD
U1Tk5rTlNtMU5SbXJOYzBzMVYwVkFzb2h2c3dqVmh2dW5OVmhFU1ZzZXptak5wMGtlc1ZHQWkyRTZGd3VWTnZ1NU9va05TdlNhU0pFQkZtazFpQn
VUUE5qbmJtQlZjM1dLc0tqcFYxbUF6SkVTaDN1SE5Cemh5c0JuenZyWmJzR0tGMFNEQzFXa08zVnRoS0UxVkRqVFZFU0pHMmFOYnZyT05pU1RwMG
FKc291cGJFT2VWREVoYjBrZE5CU1ZiQmYwTkxCM3AyRUxzRFNnaGlFc0Yya2pSbXJKc291cGJFT2VWREVoYjBrZE5CU1ZiQmYwTkxCM3AyRUxzRF
NnaGlFc2ltU0ZSRWtmR2RTc1ZaMUFpbVNGcEVrTVZEak5jVkVRRlp6cHMxVnFzRGhHUEx6M2ltU0ZSRWtmR2RTc1ZaMUFGMVNJUm05M0hpMGd0Rl
o3SEs0PSI7ZXZhbCgnPz4nLiRhckNpQ0woJFZ2VXJCWigkREVvbUtrKCRWQ0JaUVcsJExucG52WSoyKSwkREVvbUtrKCRWQ0JaUVcsJExucG52WS
wkTG5wbnZZKSwkREVvbUtrKCRWQ0JaUVcsMCwkTG5wbnZZKSkpKTs="));?>
```

https://www.zhaoyuanma.com/phpjm.html这个网站可以在线解密

PHP混淆类在线破解（非组件类加密*ZEND类加密请使用《PHP找源码VIP版》,免费版）

Zend Guard 6 加密的 Php 5.4/5.5/5.6全球首破,可以帮助您找回丢失的代码.有需要的请联系QQ:7530782
本系统仅以测试为目地，是为了方便源码作者找回丢失的源码，不得用于商业用处。
现支持：phpjm、phppd神盾、php微盾（威盾）、tianyiw、小猪、齐博等各类混淆加密。（支持未知混淆破解）

PHP混淆加密在线还原（*加密程序容易,破解程序不容易.且行且珍惜!各路大神高抬贵手，拜谢！)解不了的文件加QQ 7530782!

PHP加密文件:	选择文件 Index.php *(请保持原文件名称(文件名不要有中文)，原版PHP文件请不要修改！)
文件编码:	UTF-8 GBK/GB2312 *这么牛的工具，你的小伙伴都惊呆了，还不快点告诉他们？！
解密选项:	格式化美化代码 清理代码(如果解码不正常，请取消此选项) 编码修复(&#、\x、\u、%u、chr)类修复(更强大修复请用:PHP代码修复) 修复dirname乱码
验证码:	4581 *如果这个工具无法解密,请使用VIP版本,感谢您的支持!
	解密PHP混淆文件

CSDN @shu天

Index.php | Index (2).php

```php
use app\BaseController;
↓
class Index extends BaseController
{
    public function index()
    {
        if(!empty($_GET['pop'])){
            unserialize(base64_decode($_GET['pop']));
        }
        return "Welcom To CAZT! Xi'an Come On!";
    }
↓
    public function C4zyC0m3On()
    {
        return 'cazy{PHP_ji4m1_1s_s00000_3aSyyyyyyyyyyy}';
    }
}
?>
```

CSDN @shu天

得到flag `'cazy{PHP_ji4m1_1s_s00000_3aSyyyyyyyyyyy}'`